UNIFORM DISTRIBUTION OF POLYNOMIALS OVER $GF\{q, x\}$ IN $GF[q, x]$, PART II

BY

A. DIJKSMA

(Communicated by Prof. J. POPKEN at the meeting of February 28, 1970)

1. *Introduction*

In [2] we discussed the uniform distributivity of sequences of elements of $\Phi = GF[q, x]$, the ring of polynomials in the indeterminate x over a finite field $GF(q)$ of q elements, where $q = p^r$ for some prime number p and positive integer r. For definitions and meaning of symbols used in this paper we refer to part I. A reference to formula $(a \cdot b)$ in part I is indicated by $I(a \cdot b)$.

In this paper we prove an analogue of Van der Corput's fundamental inequality from which we derive an analogue of his well-known difference theorem (theorem (2.2)). See [1]. We remark however that lemma (2.1) and theorem (2.2) differ essentially from Van der Corput's inequality and difference theorem. For, here we have functions defined on Φ instead of I, the set of non-negative integers. Consequently theorem (2.2) is not contained in any of the generalizations of the difference theorem given by J. H. B. KEMPERMAN ([3]).

Theorem (2.2) is used in proving theorem (2.5) which states a necessary and sufficient condition for the uniform distributivity (mod 1) in $\Phi' = GF\{q, x\}$ of the sequence $\{f(Z_i)\}$, where $f(Y)$ is a polynomial over Φ' of degree k with $0 < k < p$ and $\Gamma = \{Z_i\}$ is the sequence constructed in paragraph 3 of part I.

Theorems I(3.4) and (3.4) give a necessary and sufficient condition for the uniform distributivity of the sequence $\{[f(Z_i)]\}$. It appears necessary that for the proof of the uniform distributivity in Φ of this sequence, the cases $k = 1$ and $2 \leqq k < p$ are treated separately.

Remark. It has been pointed out to the author that the domain of the exponential function e, defined in I paragraph 2, is not the whole of Φ'. To ensure that the domain of e equals Φ' we add to the definition of e: If $\alpha \in \Phi'$ and $\deg(\alpha) \leqq -2$, then $e(\alpha) = 1$.

2. *Uniform distribution in Φ' of the fractional parts of polynomials over Φ'*

Let $f(Y)$ be a polynomial over Φ' in the indeterminate Y of degree k with $0 < k < p$ (where p is the characteristic of $GF(q)$). We will show that

a necessary and sufficient condition that $\{f(Z_i)\}$ is uniformly distributed (mod 1) in Φ' is that the polynomial $f(Y)-f(0)$ has at least one irrational coefficient.

We first prove some preliminary results, one of which is the following analogue of VAN DER CORPUT's fundamental inequality ([1]).

Lemma (2.1). Let u be a complex-valued function defined on Φ. Let n and s be positive integers such that $q^s \leqq n$. If $n = aq^s + b$ where a and b are integers such that $0 \leqq b \leqq q^s - 1$, then

$$(2.1)\quad q^s(n+q^s-b)^{-1}\Big|\sum_{i=1}^{n} u(Z_i)\Big|^2 \leqq \sum_{i=1}^{n} |u(Z_i)|^2 + \sum_{h=2}^{q^s}\sum_{k=1}^{n} u(Z_k)\overline{u(Z_k+Z_h)},$$

where $u(B)=0$ if $\tau(B) \geqq n$.

Proof. If c is a non-negative integer and $cq^s \leqq \tau(Z_i) < (c+1)q^s$ then one easily verifies that $cq^s \leqq \tau(Z_i+Z_j) < (c+1)q^s$ for all integers j with $1 \leqq j \leqq q^s$. Hence, since $u(B)=0$ for $\tau(B) \geqq n$, we have

$$(2.2)\qquad q^s \sum_{i=1}^{n} u(Z_i) = \sum_{i=1}^{n+q^s-b}\sum_{j=1}^{q^s} u(Z_i+Z_j).$$

Using the Cauchy-Schwartz inequality we get from (2.2)

$$q^{2s}\Big|\sum_{i=1}^{n} u(Z_i)\Big|^2 \leqq (n+q^s-b)\sum_{i=1}^{n+q^s-b}\Big|\sum_{j=1}^{q^s} u(Z_i+Z_j)\Big|^2.$$

Consequently

$$(2.3)\quad \begin{aligned} q^{2s}(n+q^s-b)^{-1}\Big|\sum_{i=1}^{n} u(Z_i)\Big|^2 \leqq & \sum_{i=1}^{n+q^s-b}\sum_{j=1}^{q^s} |u(Z_i+Z_j)|^2 + \\ & \sum_{i=1}^{n+q^s-b}\sum_{\substack{j=1\\ j\neq l}}^{q^s}\sum_{l=1}^{q^s} u(Z_i+Z_j)\overline{u(Z_i+Z_l)} \\ = & \sum_1 + \sum_2, \end{aligned}$$

where $\sum_1$ and $\sum_2$ denote the two sums on the right-hand side.

Similar to (2.2) we have

$$(2.4)\qquad \sum_1 = q^s \sum_{i=1}^{n} |u(Z_i)|^2.$$

In $\sum_2$ terms appear which are of the form $u(Z_k)\overline{u(Z_k+Z_h)}$, $k=1, 2, \ldots, n+q^s-b$ and $h=2, 3, \ldots q^s$. Fix k and h, i.e., fix Z_k and Z_h, then if we also keep j fixed, there exist uniquely one i and one l such that $Z_i+Z_j=Z_k$

and $Z_i + Z_l = Z_k + Z_h$, viz. $Z_l = Z_k - Z_j$ and $Z_l = Z_h + Z_j$. Since j assumes exactly q^s values, we have

$$(2.5)\qquad \begin{cases} \sum_2 = q^s \sum_{h=2}^{q^s} \sum_{k=1}^{n+q^s-b} u(Z_k)\overline{u(Z_k+Z_h)} \\ \qquad = q^s \sum_{h=2}^{q^s} \sum_{k=1}^{n} u(Z_k)\overline{u(Z_k+Z_h)} \end{cases}$$

because of the fact that $u(B)=0$ if $\tau(B) \geqq n$. Substituting (2.4) and (2.5) in (2.3) and dividing by q^s, we obtain relation (2.1). This completes the proof.

Theorem (2.2). Let $g: \Phi \to \Phi'$ be a function and put $g_B(Z_i) = g(Z_i + B) - g(Z_i)$. If the sequence $\{g_B(Z_i)\}$ is uniformly distributed (mod 1) in Φ' for all $B \in \Phi$ with $B \neq 0$, then the sequence $\{g(Z_i)\}$ is uniformly distributed (mod 1) in Φ'.

Proof. Let n, s, a and b be as in lemma (2.1), and let A be an arbitrary element of $\Phi - \{0\}$. Put in (2.1) $u(Z_i) = e(Ag(Z_i))$ where e is the function defined in I paragraph 2 (see also the remark at the end of paragraph 1). Since for all $\alpha \in \Phi'$ $|e(\alpha)| = 1$ we have

$$(2.6)\qquad \sum_{i=1}^{n} |u(Z_i)|^2 = \sum_{i=1}^{n} |e(Ag(Z_i))|^2 = n$$

and

$$(2.7)\qquad \begin{cases} \overline{u(Z_k+Z_h)} = \overline{e(Ag(Z_k+Z_h))} \\ \qquad\qquad = e(-Ag(Z_k+Z_h)). \end{cases}$$

It follows from (2.7) and I(2.1) that

$$(2.8)\qquad \begin{cases} \sum_{h=2}^{q^s} \sum_{k=1}^{n} u(Z_k)\overline{u(Z_k+Z_h)} \leqq \sum_{h=2}^{q^s} \Big| \sum_{k=1}^{aq^s} u(Z_k)\overline{u(Z_k+Z_h)} \Big| + bq^s \\ \qquad\qquad = \sum_{h=2}^{q^s} \Big| \sum_{k=1}^{aq^s} e(-Ag_{Z_h}(Z_k)) \Big| + bq^s. \end{cases}$$

Substituting (2.6) and (2.8) in (2.1) and dividing by nq^s we obtain

$$n(n+q^s-b)^{-1} \Big| n^{-1} \sum_{i=1}^{n} e(Ag(Z_i)) \Big|^2 \leqq q^{-s} + q^{-s} \sum_{h=2}^{q^s} \Big| n^{-1} \sum_{k=1}^{aq^s} e(-Ag_{Z_h}(Z_k)) \Big| + bn^{-1}.$$

By the condition in the theorem and by Carlitz's criterion (see I(2.4) with $\alpha_l = g_{Z_h}(Z_i)$ and A replaced by $-A$) we have for $n \to \infty$

$$n^{-1} \sum_{k=1}^{aq^s} e(-Ag_{Z_h}(Z_k)) \to 0$$

for every $h \in \{2, 3, \ldots, q^s\}$.

Consequently

$$\lim_{n\to\infty} \sup |n^{-1} \sum_{i=1}^{n} e(Ag(Z_i))|^2 \leqq q^{-s}.$$

Since the left-hand side of this inequality is independent of s, it follows that $\lim_{n\to\infty} n^{-1} \sum_{i=1}^{n} e(Ag(Z_i)) = 0$ and thus it follows from Carlitz's criterion (see I(2.4) with $\alpha_i = g(Z_i)$) that the sequence $\{g(Z_i)\}$ is uniformly distributed (mod 1) in Φ'. This completes the proof.

Corollary (2.3). If $f(Y)$ is a polynomial over Φ' of degree k with $0 < k < p$ such that the leading coefficient of $f(Y)$ is irrational, then the sequence $\{f(Z_i)\}$ is uniformly distributed (mod 1) in Φ'.

Proof. This corollary follows from repeated application of theorem (2.2) and from theorem I(3.3). (Put in theorem I (3.3) $A_i = Z_i$ and observe that $\{Z_i\alpha\}$ is uniformly distributed (mod 1) in Φ' if and only if $\{Z_i\alpha + \beta\}$ is uniformly distributed (mod 1) in Φ', where β in Φ' is arbitrary).

Lemma (2.4). If $\alpha \in \Phi'$ is irrational and $D \in \Phi$ with $D \neq 0$, then the sequence $\{\alpha[Z_i D^{-1}]\}$ is uniformly distributed (mod 1) in Φ'.

Proof. If $\deg(D) = 0$ then $D \in GF(q) - \{0\}$ and $\alpha[Z_i D^{-1}] = D^{-1}\alpha Z_i$. Using corollary (2.3) with $f(Y) = D^{-1}\alpha Y$ we see that $\{\alpha[Z_i D^{-1}]\}$ is uniformly distributed (mod 1) in Φ'.

If $\deg(D) > 0$, then there exists a $B \in \Phi$ such that $\deg(B) < \deg(D)$ and $[\alpha + B]$ is divisible by D. Again, using corollary (2.3) with $f(Y) = (\alpha + B) D^{-1} Y$ we have by Carlitz's criterion (see I (2.4) with $\alpha_i = f(Z_i)$ and $A = 1$) for $n \to \infty$

$$\sum_{i=1}^{n} e((\alpha + B) Z_i D^{-1}) = o(n).$$

Now

$$\sum_{i=1}^{n} e((\alpha + B) Z_i D^{-1}) = \sum_{i=1}^{n} e(\alpha[Z_i D^{-1}] + B[Z_i D^{-1}] + [\alpha + B]((Z_i D^{-1})) + ((\alpha + B))((Z_i^{-1} D))).$$

Since (i) $B[Z_i D^{-1}] \in \Phi$, (ii) $[\alpha + B]((Z_i D^{-1})) \in \Phi$, because $D^{-1}[\alpha + B] \in \Phi$ and $D((Z_i D^{-1})) \in \Phi$, and (iii) $\deg(((\alpha + B))((Z_i D^{-1}))) \leqq -2$ we have

$$e(B[Z_i D^{-1}] + [\alpha + B]((Z_i D^{-1})) + ((\alpha + B))((Z_i D^{-1}))) = 1.$$

Hence by property I (2.1) we have for $n \to \infty$

$$\sum_{i=1}^{n} e(\alpha[Z_i D^{-1}]) = o(n).$$

Now, let A be an arbitrary element of $\Phi - \{0\}$. Then $A\alpha$ is irrational since

α is so. Therefore the above relation also holds for $A\alpha$ instead of α. Hence by Carlitz's criterion (see I (2.4) with $\alpha_t = \alpha[Z_t D^{-1}]$) the sequence $\{\alpha[Z_t D^{-1}]\}$ is uniformly distributed (mod 1) in Φ'. This completes the proof.

We now come to the main theorem of this paragraph.

Theorem (2.5). Let $f(Y)$ be a polynomial over Φ' of degree k with $0<k<p$. Then the sequence $\{f(Z_t)\}$ is uniformly distributed (mod 1) in Φ' if and only if the polynomial $f(Y)-f(0)$ has at least one irrational coefficient.

Proof. First assume $f(Y)=\sum_{l=0}^{k} \alpha_l Y^l (\alpha_l \in \Phi', l=0, 1, \ldots, k)$ where α_1 is the only irrational coefficient of $f(Y)-\alpha_0$. Then we may write $f(Y)=$ $=g(Y)+\alpha_1 Y+\alpha_0$, where $g(Y)$ is a polynomial over Φ' having rational coefficients only. Let D be the least common multiple of the denominators of these coefficients. Put $\deg(D)=d$. Let n be a positive integer and let a and b be two integers such that $n=aq^d+b$ and $0\leqq b\leqq q^d-1$.

Then we write

$$\sum_{i=1}^{n} e(f(Z_i)) = \sum_{i=1}^{aq^d} e(f(Z_i)) + \sum_{i=aq^d+1}^{n} e(f(Z_i))$$
$$= \sum_1 + \sum_2,$$

where $\sum_1$ and $\sum_2$ denote the two sums on the right-hand side.

Here $\sum_2 = o(n)$, $(n \to \infty)$ and

$$\sum_1 = \sum_{i=1}^{aq^d} e(g(Z_l)+\alpha_1 Z_l+\alpha_0)$$
$$= \sum_{k=0}^{a-1} \sum_{l=kq^d+1}^{(k+1)q^d} e(g(Z_l)+\alpha_1 Z_l+\alpha_0).$$

Now, if k is a non-negative integer and i is an integer such that $kq^d+1\leqq$ $\leqq i\leqq(k+1)q^d$, then

$$\{Z_l | kq^d+1\leqq l\leqq(k+1)q^d\} = \{D[Z_t D^{-1}]+Z_j | 1\leqq j\leqq q^d\}.$$

This implies

$$\sum_1 = \sum_{k=0}^{a-1} q^{-d} \sum_{i=kq^d+1}^{(k+1)q^d} \sum_{j=1}^{q^d} e(g(D[Z_t D^{-1}]+Z_j)+\alpha_1(D[Z_t D^{-1}]+Z_j)+\alpha_0).$$

It follows from the definition of D that $g(DA+B)\equiv g(B)$ (mod 1) and thus, by property I (2.2), we have $e(g(DA+B))=e(g(B))$ for all A and B in Φ. Consequently we have using I (2.1)

$$\sum_1 = q^{-d} \sum_{j=1}^{q^d} e(g(Z_j)+\alpha_1 Z_j+\alpha_0) \sum_{i=1}^{aq^d} e(\alpha_1 D[Z_t D^{-1}]).$$

It follows from lemma (2.4) with $\alpha=\alpha_1 D$ and Carlitz's criterion (see I (2.4) with $\alpha_t=\alpha_1 D[Z_t D^{-1}]$ and $A=1$) that for $n\to\infty$

$$\sum_1 = o(n).$$

Hence

$$\lim_{n\to\infty} n^{-1}\sum_{i=1}^{n} e(f(Z_i))=0. \tag{2.9}$$

Let A be an arbitrary non-zero element of Φ. Then (2.9) also holds for $Af(Z_i)$ instead of $f(Z_i)$. By Carlitz's criterion (see I (2.4) with $\alpha_i=f(Z_i)$) this implies that the sequence $\{f(Z_i)\}$ is uniformly distributed (mod 1) in Φ'.

We now proceed by induction. Suppose that if $g(Y)=\sum_{l=0}^{k}\alpha_l Y^l (\alpha_l\in\Phi'$, $l=0, 1, \ldots, k$, $0<k<p)$ where $m-1$ is the largest integral value of l such that α_l is irrational, the sequence $\{g(Z_i)\}$ is uniformly distributed (mod 1) in Φ'. Let $f(Y)=\sum_{l=0}^{k}\beta_l Y^l$ $(\beta_l\in\Phi', l=0, 1, \ldots, k)$ where m is the largest integral value of l such that β_l is irrational. Put for an arbitrary $B\in\Phi$ $f_B(Y)=f(Y+B)-f(Y)$.
Then $f_B(Y)$ is a polynomial satisfying the condition of the induction hypothesis provided that $B\neq 0$. Hence the sequence $\{f_B(Z_i)\}$ is uniformly distributed (mod 1) in Φ' for all $B\neq 0$ in Φ'. By theorem (2.2) this implies that the sequence $\{f(Z_i)\}$ is uniformly distributed (mod 1) in Φ'.

Conversely, suppose $f(Y)-f(0)$ has rational coefficients only. Let D be the least common multiple of the denominators of these coefficients.

Then $e(Df(Z_i))=e(Df(0))$ for all $Z_i\in\Phi$. Using Carlitz's criterion (see I (2.4) with $A=D$ and $\alpha_i=f(Z_i)$) we see since

$$\lim_{n\to\infty} n^{-1}\sum_{i=1}^{n} e(Df(Z_i))=e(Df(0))\neq 0$$

that the sequence $\{f(Z_i)\}$ is not uniformly distributed (mod 1) in Φ'. This completes the proof.

3. *Uniform distribution in Φ of the integral parts of polynomials over Φ'*

As a consequence of theorem (2.5) we have by corollary I (2.3) with $\alpha_i=f(Z_i)$ the following result.

Corollary (3.1). Let $f(Y)$ be defined as in theorem (2.5) and let $\{f(Z_i)\}$ be uniformly distributed (mod 1) in Φ'. Then the sequence $\{[f(Z_i)]\}$ is uniformly distributed in Φ.

In particular we have shown that the sequences $\{Z_i{}^k\alpha\}$ and $\{[Z_i{}^k\alpha]\}$ are uniformly distributed in Φ' and Φ provided that $0<k<p$ and α is irrational.

We want to extend corollary (3.1). Therefore we need two lemmas which are analogues of theorems which can be found in [4] p. 82 and p. 84 respectively. Since the proofs of these lemmas are almost identical to the ones given in [4], we will omit them here.

Lemma (3.2). Let $f(Y)$ be a polynomial over Φ of degree k with $k \geqq 1$. Then there exist infinitely many pairs (A, P) of elements of Φ with $\deg(A) < \deg(P)$ and P irreducible such that $f(A) \equiv 0 \pmod{P}$.

Lemma (3.3). Let $f(Y)$ be a polynomial over Φ of degree k with $k \geqq 1$. Let $M_i \in \Phi$, $i = 1, 2, \ldots, s$, such that $(M_i, M_j) = 1$ for $i \neq j$ $(i, j = 1, 2, \ldots, s)$. If the congruence $f(Y) \equiv 0 \pmod{M_i}$ has ν_i incongruent (mod M_i) solutions $(i = 1, 2, \ldots, s)$, then the congruence $f(Y) \equiv 0 \pmod{M}$ has $\nu_1 \nu_2 \ldots \nu_s$ incongruent (mod M) solutions, where $M = M_1 M_2 \ldots M_s$.

We now can state and prove the main theorem of this paragraph.

Theorem (3.4). Let $f(Y)$ be a polynomial over Φ' of degree k with $1 < k < p$. Then the sequence $\theta = \{[f(Z_i)]\}$ is uniformly distributed in Φ if and only if the sequence $\{f(Z_i)\}$ is uniformly distributed (mod 1) in Φ'.

Remark. The case that the degree of $f(Y)$ equals 1 has been considered in theorem I (3.4) with $A_i = f(Z_i)$, since a sequence $\{B_i\}$ is uniformly distributed in Φ if and only if the sequence $\{[B_i + \alpha]\}$ is uniformly distributed in Φ for all α in Φ'.

Proof. By an argument similar to the one used in the above remark we may suppose that $f(0) = 0$.

Corollary (3.1) proves the sufficiency. We prove the necessity by showing that if $f(Y)$ has rational coefficients only then θ is not uniformly distributed modulo some element of Φ and hence not uniformly distributed in Φ.

We first consider the case that $f(Y)$ is a monomial. Let $f(Y) = AB^{-1}Y^k$ with $B \neq 0$ and $2 \leqq k < p$. If $A = 0$ then clearly θ is not uniformly distributed in Φ. Thus we may assume that $\deg A \geqq 0$.

Put $\deg(A) = a$ and $\deg(B) = b$, and let M be any polynomial in Φ such that $m = \deg(M) \geqq 1$. Consider the congruence

$$[AB^{-1}Y^k] \equiv 0 \pmod{ABM^2}. \tag{3.1}$$

Since $k \geqq 2$, $Y = LBM$ satisfies this congruence for every L in Φ. Hence the number of solutions of (3.1) of degree less than v, where v is an integer and $v \geqq b + m$, is at least q^{v-b-m}. Consequently since $m \geqq 1$ we have

$$q^{-v}\theta(q^v, 0, ABM^2) \geqq q^{-b-m} > q^{-a-b-2m}$$

for every integer $v \geqq b + m$. This implies that

$$\limsup_{n \to \infty} n^{-1}\theta(n, 0, ABM^2) > q^{-a-b-2m}.$$

Hence the sequence θ is not uniformly distributed (mod ABM^2) in Φ.

Suppose now that $f(Y)$ is not a monomial and that $f(Y)$ has rational coefficients only. Let $D \in \Phi$ be a common multiple of the denominators of these coefficients. Put $d = \deg(D)$. Without loss of generality we may assume $d > 0$. Then we may write $f(Y) = D^{-1} g(Y) Y^s$ with $s \geqq 1$, $g(Y)$ a polynomial (not a monomial) over Φ, and $g(0) \neq 0$. Let u be an integer such that $2^u \geqq q^{d+1}$.

According to lemma (3.2) there exist infinitely many pairs (A, P) of polynomials in Φ with $\deg(A) < \deg(P)$ and P irreducible such that $g(A) \equiv 0 \pmod{P}$. Consider u such pairs (A_j, P_j) with the additional condition that $\deg(P_j) > \max(d, \deg(g(0)))$, $j = 1, 2, \ldots, u$. Then $A_j \neq 0$ for all $j = 1, 2, \ldots, u$, for otherwise $g(0) = 0$ which is not true. Consequently for each $j = 1, 2, \ldots, u$ there exist at least two incongruent (mod P_j) solutions of the congruence $g(Y) Y^s \equiv 0 \pmod{P_j}$, viz. $Y = 0$ and $Y = A_j$.

Furthermore, $Y = 0$ is a solution of the congruence $g(Y) Y^s \equiv 0 \pmod{D}$. Since P_j is irreducible and $\deg(P_j) > d$ for each $j = 1, 2, \ldots, u$, each two different polynomials of the set $\{P_1, P_2, \ldots, P_u, D\}$ are relatively prime. We now apply lemma (3.3) with $s = u + 1$, $M_j = P_j$ and $\nu_j = 2$ $(j = 1, 2, \ldots, u)$, $M_s = D$ and $\nu_s = 1$, and $M = P_1 P_2 \ldots P_u D$ and conclude that the congruence $g(Y) Y^s \equiv 0 \pmod{P_1 P_2 \ldots P_u D}$ has at least 2^u incongruent (mod $P_1 P_2 \ldots P_u D$) solutions. Put $P = P_1 P_2 \ldots P_u$ and let $t = \deg(P)$. Since $f(Y) = D^{-1} g(Y) Y^s$ we see that the congruence

$$[f(Y)] \equiv 0 \pmod{P} \tag{3.2}$$

has at least 2^u incongruent (mod PD) solutions. Hence, if v is an integer such that $v \geqq t + d$, then the number of solutions of (3.2), which are of degree less then v, is at least $2^u q^{v-t-d}$. This implies that

$$q^{-v} \theta(q^v, 0, P) \geqq 2^u q^{-t-d}.$$

Since $2^u > q^{d+1}$ it follows that

$$\limsup_{n \to \infty} n^{-1} \theta(n, 0, P) \geqq q^{-t+1} > q^{-t}.$$

Hence θ is not uniformly distributed (mod P) in Φ. This completes the proof.

Remark. The restrictions $\deg(f(Y)) < p$ in theorems (2.5) and (3.4) cannot be omitted. We will show that there exists an irrational α in Φ' such that the sequence $\{\alpha Z_i^p\}$ is not uniformly distributed (mod 1) in Φ' and such that the sequence $\{[x \alpha Z_i^p]\}$ is not uniformly distributed (mod x) in Φ.

Let $\alpha = \sum_{j=1}^{\infty} x^{-p^j}$. Then α is algebraic and satisfies the equation $x^p Y^p - x^p Y + 1 = 0$. It is not difficult to show that this equation has no rational

solutions in Φ'. Hence α is irrational. Let $Z \in \Phi$ be arbitrary and put $Z = \sum_{l=0}^{k} a_l x^l$ where $a_l \in GF(q)$, $l = 0, 1, \ldots, k$. Then $Z^p = \sum_{l=0}^{k} (a_l)^p x^{pl}$ and $\alpha Z^p = \sum_{j=1}^{\infty} \sum_{l=0}^{k} (a_l)^p x^{-p^j+pl}$. Since $-p^j+pl \equiv 0 \pmod{p}$ for all $j \geqq 1$ and $l \geqq 0$, we see that $-p^j+pl \neq -1$ for all $j \geqq 1$ and $l \geqq 0$. Hence the coefficient of x^{-1} of αZ^p equals zero for all $Z \in \Phi$. This implies that for all non-negative integers i

$$e(\alpha Z_i^p) = 1.$$

Carlitz's criterion (see I (2.4) with $A = 1$ and $\alpha_i = \alpha Z_i^p$) now implies that the sequence $\{\alpha Z_i^p\}$ is not uniformly distributed (mod 1) in Φ'.

Since $\deg(x^{-1}((x\alpha Z_i^p))) \leqq -2$ we have by property I (2.1)

$$\begin{aligned} e(x^{-1}[x\alpha Z_i^p]) &= e(\alpha Z_i^p) e(-x^{-1}((x\alpha Z_i^p))) \\ &= e(\alpha Z_i^p) \\ &= 1. \end{aligned}$$

It follows from theorem I (2.1) that the sequence $\{[x\alpha Z_i^p]\}$ is not uniformly distributed (mod x) in Φ.

University of Technology, Delft

REFERENCES

1. Corput, J. G. van der, Diophantische Ungleichungen I, Acta Mathematica, **56**, 373–456 (1931).
2. Dijksma, A., Uniform distribution of polynomials over $GF\{q, x\}$ in $GF[q, x]$, part I, Nederl. Akad. Wetensch. Proc. Ser. A, **72**, 4, 376–383 (1969) = Indag. Math., **31**, 4, 376–383 (1969).
3. Kemperman, J. H. B., On the distribution of a sequence in a compact group, Comp. Math., **16**, 138–157 (1964).
4. Nagell, T., Introduction to number theory, New York, John Wiley, (1951).